IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

REBEKAH LOCKHART and **JAMES LOWE**, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	Case No. 5:23-cv-01156
v.	)	
EL CENTRO DEL BARRIO d/b/a **CENTROMED,**	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Rebekah Lockhart and James Lowe ("Plaintiffs"), by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, file this complaint against El Centro Del Barrio d/b/a CentroMed ("CentroMed" or "Defendant") and allege the following:

NATURE OF THE ACTION

1. Plaintiffs bring this class action complaint on behalf of a class of persons impacted by Defendant's failure to safeguard, monitor, maintain and protect highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information"). Defendant collected, stored, and maintained its current and former patients' and employees', including Plaintiffs' and Class Members', Sensitive Information as part of its employment practices and provision of healthcare services to patients.

2. On or around June 12, 2023, CentroMed learned that its networks containing its patients' and employees' Sensitive Information were impacted during a cyberattack (the "Data Breach"). Specifically, Defendant determined that on June 9, 2023, hackers accessed Defendant's systems and "files that contain information pertaining to CentroMed's current and former patients,

employees, providers, and employee and provider spouses / partners / dependents."[1] Defendant disclosed that its Data Breach exposed current and former patients' Sensitive Information, including name, address, date of birth, Social Security number (SSN) financial account information, medical records number, health insurance plan member ID, and claims data (including diagnoses listed on claims).[2] Additionally, Defendant disclosed that its Data Breach exposed current and former employees' or providers', along with those employees' or providers' spouses', partners', and/or dependents', Sensitive Information, including name, SSN, financial account information, health insurance plan member ID, and claims data.[3]

3. Although Defendant discovered the Data Breach on or around June 12, 2023, it inexplicably waited until on or around August 11, 2023, approximately two months later, to purportedly begin issuing direct notice to the patients, employees, and other individuals impacted by the Data Breach. In its online Data Breach notice, Defendant admitted that its networks and systems had been breached and that the cyberattack exposed highly sensitive information.

4. The type of information impacted by the Data Breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. Indeed, the entire purpose of these types of medical data breaches is to misuse the stolen information or to sell it to fraudsters on the dark web. Consequently, all impacted individuals are at a heightened and significant risk that their information will be disclosed to criminals and misused for attempted or actual fraud or identity theft.

---

[1] *Notice of Data Security Incident*, CENTROMED, https://centromedsa.com/wp-content/uploads/2023/08/Notice_2023_Aug_11_2023l.pdf (last visited Sept. 12, 2023).

[2] *Id.*

[3] *Id.*

5. As a result of Defendant's lax data security concerning its systems and servers, hundreds or thousands of Defendant's patients and employees have had sensitive details of their lives and identities accessed, viewed and stolen by malicious cybercriminals. These patients have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

6. Defendant's conduct, consequently, required Plaintiffs and Class Members to have to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Sensitive Information, including by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions and health insurance providers, closing or modifying financial accounts, reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records.

7. As such, Plaintiffs and Class Members bring this action to recover for the harm they suffered and assert the following claims: (I) Negligence, (II) Negligence Per Se, (III) Breach of Implied Contract, (IV) Unjust Enrichment, (V) Breach of Fiduciary Duty, (VI) Violation of the Texas Medical Practice Act, and (VII) Violation of the Texas Hospital Licensing Law.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant El Centro Del Barrio d/b/a CentroMed. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

9. This Court has personal jurisdiction over Defendant because its principal place of business is located in the San Antonio Division of the Western District of Texas, and Defendant conducts substantial business within this District.

10. Venue is proper under 28 U.S.C. § 1391(b) because Defendant maintains its principal place of business within the San Antonio Division of the Western District of Texas and because a substantial part of the acts or omissions giving rise to this action occurred within this District.

THE PARTIES

11. Plaintiff Rebekah Lockhart is a natural person and citizen of Texas, residing in Converse, Texas. She is a current patient of CentroMed and received healthcare services from Defendant. Plaintiff Lockhart provided Defendant with her sensitive PII and PHI for purposes of receiving healthcare services. She received a Data Breach Notice Letter on or around August 11, 2023, informing her that her Sensitive Information was part of Defendant's Data Breach, including her name, address, date of birth, Social Security number (SSN) financial account information, medical records number, health insurance plan member ID, and claims data (including diagnoses listed on claims).

12. Plaintiff James Lowe is a natural person and citizen of the State of Texas, residing in San Antonio, Texas. He is a current patient of Defendant and received healthcare services from Defendant. Plaintiff Lowe provided Defendant with his sensitive PII and PHI for purposes of receiving healthcare services. He received a Data Breach Notice Letter on or around August 11, 2023, informing him that his Sensitive Information was part of Defendant's Data Breach, including his name, address, date of birth, Social Security number (SSN) financial account information,

medical records number, health insurance plan member ID, and claims data (including diagnoses listed on claims).

13. Defendant El Centro Del Barrio d/b/a CentroMed is a healthcare company incorporated under the laws of the State of Texas. Defendant maintains its principal place of business at 3750 Commercial Avenue, San Antonio, Texas 78221. The registered agent for service of process is Ernesto Gomez at 3750 Commercial Avenue, San Antonio, Texas 78221.

COMMON FACTUAL ALLEGATIONS

A. Defendant Collected, Maintained and Stored Sensitive Information

14. Defendant is a Texas-based healthcare facility that provides a variety of services to its patients, including medical services, dental services, and behavioral health therapy.[4]

15. Plaintiffs and Class Members are current and former CentroMed patients and/or current and former CentroMed employees and/or dependents or spouses of current and former CentroMed patients and employees.

16. As an ordinary and regular part of the medical and/or employment services that it provides to its patients and/or employees, Defendant collects, creates, and maintains patients' and employees' Sensitive Information. Defendant's Notice of Data Breach, posted online, claims that "El Centro Del Barrio . . . is committed to protecting the security and privacy of the information we maintain."[5]

17. As a prerequisite to receiving healthcare services and/or obtaining employment with Defendant, Defendant requires its patients and employees to provide it with their Sensitive Information. Defendant maintains patients' name, address, date of birth, Social Security number

[4] *Services*, CENTROMED, https://centromedsa.com/services/ (last visited Sept. 12, 2023).

[5] *Notice of Data Security Incident*, *supra* note 1.

(SSN) financial account information, medical records number, health insurance plan member ID, and claims data (including diagnoses listed on claims). Defendant further maintains its employees', along with those employees' spouses', partners', and dependents', name, SSN, financial account information, health insurance plan member ID, and claims data.

18. The PHI and PII that Defendant maintains is highly sensitive. To obtain healthcare services and/or employment, patients and employees, like Plaintiffs and Class Members, must provide Defendant with highly sensitive information, including PHI, PII, or both. As a sizable healthcare services provider, Defendant has collected and maintained a depository of Sensitive Information, a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.

19. Plaintiffs and Class Members had a reasonable expectation that Defendant would protect the Sensitive Information that it collected and maintained, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect Plaintiffs' and Class Members' Sensitive Information could cause substantial harm.

20. Defendant's Privacy Policy acknowledges the sensitivity of the information that it maintains, along with the legal requirements for Defendant to confidentially maintain such information.

21. Specifically, Defendant's Notice of Client Privacy Rights provides:

> This notice applies to all of the records of your care generated by this Center, whether made by the Center or an associated provider. Our policies on protecting your health information extend to all professional authorized persons who have a need to know to provide care to you. The policies apply to all areas of the Center including all Center staff, the front desk, billing and administration. It also applies to any entity or individual with whom we contract services, such as referral providers.

> **Your Protected Health Information**
> As our patient, we create paper and electronic medical records and documents concerning you and your health, as well as the care and services we provide to you. We need this record to provide continuity of care and to comply with certain legal requirements. We are required by law to:
>
> • make sure that your protected health information is kept private,
>
> • provide you with this Notice of Client Privacy Rights, containing our legal duties and privacy practices with respect to protected health information,
>
> • follow the terms of this Notice currently in effect and make sure the law and your legal rights are in effect[,]
>
> • to inform you that your protected health information is subject to electronic disclosure for purposes that are permitted or required by law, and
>
> • to notify affected individuals following a breach of unsecured protected health information.[6]

22. Plaintiffs and Class Members relied on Defendant's representations that their Sensitive Information would be secure before purchasing healthcare services from Defendant and/or obtaining employment with Defendant.

23. In purchasing healthcare services and/or obtaining employment from Defendant, Plaintiffs and Class Members relied on Defendant to keep their Sensitive Information confidential and securely maintained.

24. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiffs' and Class Members' Sensitive Information prior to, during, or after the Data Breach, but rather enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant

[6] *Notice of Client Privacy Rights*, CENTROMED (Aug. 2013), https://centromedsa.com/wp-content/uploads/2016/11/notice_of_clients_privacy_rights_eng-span-1.pdf.

maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

B. Defendant's Data Breach Exposed Patients' Sensitive Information

25. On June 12, 2023, Defendant discovered suspicious activity on its systems. Defendant claims to have initiated an investigation and taken containment measures at that point, but those measures were clearly insufficient. Defendant later admitted that third-party hackers had gained access to its systems and to the highly sensitive PII and PHI of Plaintiffs and Class Members. Upon information and belief, during the Data Breach, the hackers copied and/or exfiltrated substantial amounts of Plaintiffs' and Class Members' Sensitive Information.

26. Defendant waited approximately two months to start providing notice to the individuals impacted by the Data Breach. Specifically, despite identifying the Data Breach on June 12, 2023, Defendant did not notify Plaintiffs and Class Members of the compromise of their Sensitive Information until on or around August 11, 2023. A delay of two months is patently unreasonable and put Plaintiffs and Class Members at a continued and significant risk of harm that their stolen data, capable of being used for medical, insurance, or financial fraud and identity theft, would be misused. Had Defendant provided notice sooner, Plaintiffs and Class Members would have been able to take mitigatory steps sooner.

27. In its Notice of Data Breach, Defendant states:

> El Centro Del Barrio d/b/a CentroMed ("CentroMed") is committed to protecting the security and privacy of the information we maintain. We recently responded to and addressed a data security incident that involved patient information. This notice explains the incident, the measures that have been taken, and some steps patients can take in response.
>
> **What Happened:**
>
> On June 12, 2023, we were alerted to potential unauthorized access to our information technology ("IT") network. Upon learning of this, we immediately

> launched an investigation. The investigation determined that an unauthorized party accessed some of our systems on June 9, 2023. While in our IT network, the unauthorized party accessed files that contain information pertaining to CentroMed's current and former patients, employees, and employee and provider spouses / partners / dependents. Our investigation cannot rule out the possibility that, as a result of this incident, files containing some of your information may have been subject to unauthorized access.
>
> **What Information is Involved:**
>
> If you are a patient: your name, address, date of birth, Social Security number, financial account information, medical records number, health insurance plan member ID, and claims data (including diagnoses listed on claims) may have been involved.
>
> If you are a current or former employee or provider: your name, Social Security number, financial account information, health insurance plan member ID, and claims data may have been involved.
>
> If you are a spouse/partner or dependent of a current or former employee or provider: your name, Social Security number, financial account information, health insurance plan member ID, and claims data may have been involved.[7]

28. Defendant identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in the Notice of Data Breach:

> **Steps We Are Taking:**
>
> On August 11, 2023, CentroMed began providing notice to individuals whose information may have been involved in the incident. In addition, CentroMed established a dedicated, toll-free call center to answer questions that individuals may have. We take this incident very seriously and sincerely regret any concern this may cause. To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures to further protect and monitor our systems.[8]

29. Defendant recognized the substantial and high likelihood that Plaintiffs' and Class Members' Sensitive Information would be misused, instructing affected individuals:

> **Steps You Can Take:**

---

[7] *Notice of Data Security Incident*, *supra* note 1.

[8] *Id.*

> For patients whose information may have been involved in the incident, we recommend reviewing the statements they receive from their healthcare providers and contacting the relevant provider immediately if they see services they did not receive. We also encourage patients and others to remain vigilant to the possibility of fraud by reviewing their financial account statements for any suspicious activity. Patients should immediately report any suspicious activity to your financial institution.[9]

30. Defendant largely put the burden on Plaintiffs and Class Members to take measures to protect themselves.

31. Given that Defendant was storing the Sensitive Information of Plaintiffs and Class Members and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient and employee records and data and, additionally, because other highly publicized data breaches at numerous healthcare institutions put Defendant on notice that the personal and sensitive data they stored might be targeted by cybercriminals.

32. Indeed, cyberattacks on medical systems and healthcare companies like Defendant have become so notorious that the Federal Bureau of Investigation and United States Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are

[9] *Id.*

attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

33. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in recent years.[11]

34. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

35. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of healthcare data breaches, Defendant inexplicably failed to adopt sufficient data security processes by, without limitation:

a. Failing to properly select its information security partners;

b. Failing to ensure the proper monitoring and logging of the ingress and egress of network traffic;

c. Failing to ensure the proper monitoring and logging of file access and modifications;

d. Failing to ensure the proper training its and its technology partners' employees as to cybersecurity best practices;

e. Failing to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members;

---

[10] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[11] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

f. Failing to timely and accurately disclose that Plaintiffs' and Class Members' PII and PHI had been improperly acquired or accessed;

g. Knowingly disregarding standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI; and

h. Failing to provide adequate supervision and oversight of the PII and PHI with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and PHI of Plaintiffs and Class Members, misuse the PHI/PII and potentially disclose it to others without consent.

36. Upon information and belief, Defendant further failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data security incidents, to ensure the proper encryption of Plaintiffs' and Class Members' Sensitive Information, and to monitor user behavior and activity to identify possible threats.

37. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

38. Despite the highly sensitive nature of the information Defendant obtained, maintained, and stored and the prevalence of health care data breaches, Defendant inexplicably failed to take appropriate steps to safeguard the Sensitive Information of Plaintiffs and Class Members from being compromised. The Data Breach itself, and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information it oversaw.

C. Defendant Failed to Comply with FTC Guidelines

39. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[12]

40. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of

[12] Pamela Jones Harbour, Commissioner, Fed. Trade Comm'n, Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[13] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[15]

43. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

---

[13] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[14] *Id*.

[15] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[16]

44. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[17] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. These FTC enforcement actions include actions against healthcare providers and partners like Defendant.[18]

47. Defendant failed to properly implement basic data security practices.

---

[16] *Id.*

[17] *See* FED. TRADE COMM'N, TAKING CHARGE, WHAT TO DO IF YOUR IDENTITY IS STOLEN at 3 (2012), *available at* https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf.

[18] *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

48. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Defendant was at all times fully aware of the obligation to protect the Sensitive Information of customers, patients, and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Defendant Failed to Comply with Industry Standards

50. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

51. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

52. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

53. Other best cybersecurity practices that are standard in the healthcare industry

include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

54. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1[19] (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls[20] (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

55. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

56. Defendant did not rapidly, or even reasonably, report to Plaintiffs and Class Members that their Sensitive Information had been exposed or stolen. Instead, Defendant waited approximately two months after identifying the Data Breach before notifying Plaintiffs and Class Members of the Data Breach.

---

[19] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[20] *See The 18 CIS Critical Security Controls*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-list (last visited May 11, 2023).

57. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

E. Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

58. The Health Insurance Portability and Accountability Act ("HIPAA") requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

59. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PII and PHI. Safeguards must include physical, technical, and administrative components.[21]

60. Title II of HIPAA contains what are known as the Administrative Simplification provisions.[22] These provisions require, among other things, that the Department of Health and Human Services ("DHHS") create rules to streamline the standards for handling PII and PHI, like the data Defendant left unguarded. The DHHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1)–(4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

61. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI

[21] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

[22] 42 U.S.C. §§ 1301, *et seq*.

in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[23]

62. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

F. Defendant Violated Standards Set Forth in Texas Law

63. The Texas Medical Practice Act ("TMPA"), Tex. Occ. Code §§ 159.001, *et seq.*, prohibits the unauthorized disclosure of communications between a physician and a patient and records of the identity, diagnosis, evaluation, or treatment of a patient by a physician.[24]

64. Furthermore, persons, including hospitals, that receive information from a confidential communication or record, as described above, "may not disclose the information except to the extent that disclosure is consistent with the authorized purposes for which the information was first obtained."[25]

65. The Texas Hospital Licensing Law ("THLL"), Tex. Health & Safety Code §§ 241.001, *et seq.*, also prohibits a hospital or an agent or employee of a hospital from "disclos[ing] health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative."[26]

---

[23] *See* 45 C.F.R. § 164.40.

[24] *See* TEX. OCC. CODE § 159.002(a)–(b).

[25] *Id.* § 159.002(c).

[26] TEX. HEALTH & SAFETY CODE § 241.152(a).

66. As used in the THLL, "health care information" means "information, including payment information, recorded in any form or medium that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient."[27]

67. The THLL further requires hospitals to "adopt and implement reasonable safeguards for the security of all health care information it maintains."[28]

68. Defendant's Data Breach and unauthorized disclosure of Plaintiffs' and Class Members' Sensitive Information to malicious third parties violated Plaintiffs' and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standards for safeguard the confidential Sensitive Information of Plaintiffs and Class Members.

G. Defendant's Data Breach

69. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and employees' Sensitive Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

[27] *Id.* § 241.151(2).

[28] *Id.* § 241.155.

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to train its employees in the proper handling of emails containing Sensitive Information and maintain adequate email security practices;

i. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

j. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

k. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

l. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

m. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

n. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

o. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

p. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key;"[29]

r. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

s. Failing to adhere to industry standards for cybersecurity as discussed above; and

t. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Sensitive Information.

70. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Sensitive Information. Accordingly, as outlined below, Plaintiffs and Class Members now face actual fraud and identity theft as well as increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members lost the benefit of the bargain they made with Defendant.

[29] 45 C.F.R. § 164.304.

H. Cyberattacks and Data Breaches Cause Disruption and Put Victims at an Increased Risk of Fraud and Identity Theft

71. Cyberattacks and data breaches at healthcare companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

72. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[30]

73. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[31]

74. The United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in

---

[30] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[31] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RES. 971, 971–80 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[32] *See* U.S. Gov. Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 2 (2007), *available at* https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

76. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

77. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

78. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social

[33] *See IdentityTheft.gov*, FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited May 18, 2023).

Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

79. Moreover, theft of Sensitive Information is also gravely serious because Sensitive Information is an extremely valuable property right.[34]

80. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Sensitive Information has considerable market value.

81. Theft of PHI, in particular, is gravely serious. A thief may use customers' and patients' name or health insurance numbers "to see a doctor, get prescription drugs, buy medical devices, submit claims with [an] insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to sue. It could also hurt your credit."[35]

82. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Sensitive Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to

---

[34] *See, e.g.,* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J. L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[35] *What To Know About Medical Identity Theft*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft#:~:text=Medical%20identity%20theft%20is%20when,or%20get%20other%20medical%20care (last visited May 18, 2023).

adjust their insureds' medical insurance premiums.

83. There may additionally be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Sensitive Information and/or financial information is stolen and when it is used.

84. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[36]

85. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

86. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

87. Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

88. Sensitive Information can sell for as much as $363 per record according to the Infosec Institute.[37] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims

---

[36] GAO Report, *supra* note 32, at 29.

[37] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

may continue for years.

89. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[39] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

91. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[40]

92. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

[38] Soc. Sec. Admin., Pub. No. 05-10064, *Identity Theft and Your Social Security Number* 1 (2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

[39] *Id.* at 4.

[40] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[41]

93. Medical information is especially valuable to identity thieves.

94. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[42] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[43]

95. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

96. For this reason, Defendant knew or should have known about these dangers and strengthened its data systems and data security measures accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

I. Plaintiffs' and Class Members' Damages

97. Plaintiffs and Class Members have been damaged by the compromise of their Sensitive Information in the Data Breach.

98. Plaintiffs' and Class Members' Sensitive Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed the data Defendant held within

---

[41] Tim Greene, *Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers*, NETWORKWORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[42] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LOGDOG (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[43] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

its systems. The Sensitive Information exposed included "the names, addresses, dates of birth, SSNs, medical record numbers and account numbers, and diagnostic codes used to identify diagnoses and treatments of current and former healthcare patients" of Defendant, along with "the names, addresses, SSNs, and dates of birth of current and former employees [of Defendant] and their dependents and beneficiaries."[44]

99. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

100. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach, valuable time Plaintiffs and Class Members otherwise would have spent on other activities, including but not limited to work and/or recreation.

101. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

102. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Sensitive Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

103. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

[44] *Notice of Cybersecurity Incident*, *supra* note 1.

104. Plaintiffs and Class Members also suffered a loss of value of their Sensitive Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

105. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members who are current or former patients of Defendant overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate data security practices to safeguard Plaintiffs' and Class Members' Sensitive Information. As demonstrated by the Data Breach, Defendant failed to fund and provide adequate data security practices. Thus, Plaintiffs and the Class Members who are current or former patients of Defendant did not get what they paid for and agreed to.

106. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably spent to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring their SSN, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

107. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Sensitive Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Sensitive Information is not accessible online or otherwise to unauthorized third parties.

108. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Sensitive Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

109. As a direct and proximate result of Defendant's actions and omissions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

J. Plaintiffs' Experiences

i. Plaintiff Rebekah Lockhart's Experience

110. Plaintiff Lockhart is a resident and citizen of Texas. Plaintiff Lockhart is a current patient of Defendant.

111. As a condition of receiving healthcare services, Defendant required Plaintiff Lockhart to provide the company with her Sensitive Information.

112. Plaintiff Lockhart provided Defendant with her Sensitive Information in order to purchase and receive healthcare services.

113. On or about August 11, 2023, Plaintiff Lockhart received a Notice of Data Breach from Defendant, which informed her of the Data Breach and that she faced a substantial and significant risk of her Sensitive Information being misused. The Notice informed Plaintiff that her Sensitive Information had been improperly accessed and/or obtained by unauthorized third parties. The Notice indicated that Plaintiff's Sensitive Information was compromised as a result of the Data Breach.

114. Plaintiff Lockhart reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Sensitive Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same. Plaintiff Lockhart would not have used Defendant's services had she known that Defendant would not take reasonable steps to safeguard her Sensitive Information.

115. Shortly after, and as a result of the Data Breach, Plaintiff Lockhart has experienced a significant increase in spam calls and emails, indicating that her Sensitive Information, including confidential medical information, has been compromised and is now subject to misuse by unidentified, malicious third parties.

116. Plaintiff Lockhart is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Lockhart stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

117. As a result of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff Lockhart made reasonable efforts to mitigate the impact of the Data Breach,

including but not limited to researching the Data Breach, reviewing financial statements, monitoring her credit information, and changing passwords on her various accounts.

118. Plaintiff Lockhart has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

119. Plaintiff Lockhart suffered actual injury from having her sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) entrusting PII and PHI to Defendant that she would not have had Defendant disclosed it lacked data security practices adequate to safeguard its patients' and employees' Sensitive Information; (b) damages to and diminution in the value of her Sensitive Information–a form of intangible property that she entrusted to Defendant as a condition of receiving healthcare benefits services; (c) loss of her privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of her mitigation efforts as a result of the Data Breach.

120. Due to the Data Breach, Plaintiff Lockhart anticipates spending considerable additional time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, monitoring her medical history and health insurance information, and monitoring her other accounts for fraudulent activity.

121. In addition, knowing that hackers accessed and/or stole her PII and PHI to commit fraud and identity theft and that this will likely be used in the future for identity theft, fraud, and related purposes has caused Plaintiff Lockhart to experience feelings of rage, anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or

inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

122. Plaintiff Lockhart suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her PII and PHI.

123. Plaintiff Lockhart is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties/criminals.

124. Plaintiff Lockhart has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

ii. Plaintiff James Lowe's Experience

125. Plaintiff Lowe is a resident and citizen of Texas. Plaintiff Lowe is a current patient of Defendant.

126. As a condition of receiving healthcare services, Defendant required Plaintiff Lowe to provide the company with his Sensitive Information.

127. Plaintiff Lowe provided Defendant with his Sensitive Information in order to purchase and receive healthcare services.

128. On or about August 11, 2023, Plaintiff Lowe received a Notice of Data Breach from Defendant, which informed him of the Data Breach and that he faced a substantial and significant risk of his Sensitive Information being misused. The Notice informed Plaintiff that his Sensitive Information had been improperly accessed and/or obtained by unauthorized third parties. The

Notice indicated that Plaintiff's Sensitive Information was compromised as a result of the Data Breach.

129. Plaintiff Lowe reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard his Sensitive Information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to the same. Plaintiff Lowe would not have used Defendant's services had he known that Defendant would not take reasonable steps to safeguard his Sensitive Information.

130. Shortly after, and as a result of the Data Breach, Plaintiff Lowe experienced actual fraud and/or identity theft when he received notification of a loan application completed using his information that he neither submitted nor authorized. Additionally, since the Data Breach, Plaintiff has experienced an increase in spam calls and spam emails related to loans he did not inquire about.

131. Plaintiff Lowe is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Lowe stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

132. As a result of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff Lowe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial statements, monitoring his credit information, and handling the fraudulent loan application submitted using his information.

133. Plaintiff Lowe has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

134. Plaintiff Lowe suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) actual fraud and identity theft; (b) entrusting PII and PHI to Defendant that he would not have had Defendant disclosed it lacked data security practices adequate to safeguard its patients' and employee's Sensitive Information; (c) damages to and diminution in the value of his Sensitive Information–a form of intangible property that he entrusted to Defendant as a condition of receiving healthcare benefits services; (d) loss of his privacy; (e) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (f) time and expense of his mitigation efforts as a result of the Data Breach.

135. Due to the Data Breach, Plaintiff Lowe anticipates spending considerable additional time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, monitoring his medical history and health insurance information, and monitoring his other accounts for fraudulent activity.

136. In addition, knowing that hackers accessed and/or stole his PII and PHI to commit fraud and identity theft and that this will likely be used in the future for identity theft, fraud, and related purposes has caused Plaintiff Lowe to experience feelings of rage, anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

137. Plaintiff Lowe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI.

138. Plaintiff Lowe is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties/criminals.

139. Plaintiff Lowe has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

140. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23 on behalf of themselves and all others similarly situated (the "Class") defined as:

> All individuals residing in the United States whose PII and/or PHI was impacted by the Data Breach, including all persons to whom Defendant sent a notice of the Data Breach.

141. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

142. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as the case progresses.

143. **Numerosity:** The exact number of members of the Class is unknown but, upon information and belief, it is estimated to number in the tens or hundreds of thousands at this time, and individual joinder in this case is impracticable. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

144. **Typicality:** Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs, and the members of the Class, sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

145. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiffs.

146. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendant violated the laws asserted herein, including statutory privacy laws;

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiffs' and members of the Class's Sensitive Information;

c. Whether Defendant breached the duty to use reasonable care to safeguard Plaintiffs' and members of the Class's Sensitive Information;

d. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's Sensitive Information;

e. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing Sensitive Information;

f. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and members of the Class's Sensitive Information from unauthorized release and disclosure;

g. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Class's Sensitive Information from unauthorized release and disclosure;

h. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;

j. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;

k. Whether Defendant's conduct was likely to deceive the public;

l. Whether Defendant is liable for negligence or gross negligence;

m. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the Sensitive Information violated applicable state laws;

n. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;

o. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiffs and members of the Class;

p. Whether Defendant's practices and representations related to the Data Breach breached implied contracts with Plaintiffs and members of the Class;

q. What the proper measure of damages is; and

r. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

147. **Superiority:** This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties

and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

148. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

149. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Sensitive Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

150. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

Count I
Negligence
(On Behalf of Plaintiffs and the Class)

151. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

152. Defendant required its patients and employees, including Plaintiffs and Class Members, to submit their Sensitive Information to receive Defendant's services and/or obtain employment with Defendant.

153. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiffs' and Class Members' Sensitive Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by

which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

154. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, the personnel responsible for them, and its information technology partners adequately protected the Sensitive Information.

155. Plaintiffs and the Class are a well-defined, foreseeable, and probable group of patients and employees that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

156. A large repository of highly valuable healthcare and personal information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Sensitive Information for thousands of patients and/or employees posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard Plaintiffs' and Class Members' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

157. After all, PII and PHI are highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiffs and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the Sensitive Information entrusted to them.

158. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its patients and/or employees, which

is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

159. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[45] Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

160. In addition, Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.[46]

161. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

162. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Sensitive Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Sensitive Information;

b. Failing to adequately monitor the security of its networks and systems;

[45] 45 C.F.R. § 164.530(c)(1).

[46] *See* 15 U.S.C. § 45.

c. Failing to have in place mitigation policies and procedures;

d. Allowing unauthorized access to Plaintiffs' and Class Members' Sensitive Information;

e. Failing to detect in a timely manner that Plaintiffs' and Class Members' Sensitive Information had been compromised; and

f. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

163. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiffs' and Class Members' Sensitive Information.

164. The failure of Defendant to comply with industry standards and federal regulations evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Sensitive Information.

165. But for Defendant's wrongful and negligent breach of its duties to Plaintiffs and Class Members, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiffs and Class Members and all resulting damages.

166. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' Sensitive Information would result in injury to Plaintiffs and Class

Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

167. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Sensitive Information would result in one or more types of injuries to Plaintiffs and Class Members.

168. As a result of this misconduct by Defendant, the Sensitive Information of Plaintiffs and Class Members was compromised, placing them at a greater risk of identity theft and of their Sensitive Information being disclosed to third parties without the consent of Plaintiffs and the Class.

169. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

170. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to Plaintiffs and all Class Members.

Count II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

171. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

172. Plaintiffs allege this negligence *per se* theory as alternative to Count I.

173. Pursuant to the laws set forth herein, including the TMPA, Tex. Occ. Code §§ 159.001, *et seq.*, the THLL, Tex. Health & Safety Code §§ 241.001, *et seq.*, the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E

("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Sensitive Information.

174. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Sensitive Information. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[47]

175. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

176. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Sensitive Information. Defendant had a duty to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[48] Some

[47] 15 U.S.C. § 45.

[48] 45 C.F.R. § 164.530(c)(1).

or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.[49]

177. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[50]

178. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect. And the injuries that Defendant inflicted on Plaintiffs and Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses which—because of their failure to employ reasonable data security measures for PHI— caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

179. Under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Defendant has a duty to promptly notify "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach" the respective covered entities and affected persons so that the entities and persons can take action to protect themselves.[51]

180. Moreover, the HITECH states that, "[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured

---

[49] *Id.*

[50] *See id.* § 164.304.

[51] 42 U.S.C. § 17932(d)(1).

protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach."[52]

181. The HITECH further provides, "[a] business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."[53]

182. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

183. Defendant owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Defendant's Data Breach.

184. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

[52] *Id.* § 17932(a).

[53] *Id.* § 17932(b).

or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the Sensitive Information of Plaintiffs and Class Members.

185. Defendant breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Sensitive Information. And but for Defendant's negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Sensitive Information;
b. Failing to comply with—and thus violating—HIPAA and its regulations;
c. Failing to comply with—and thus violating—HITECH and its regulations;
d. Failing to comply with—and thus violating—FTCA and its regulations;
e. Failing to comply with—and thus violating—the TMPA and its regulations;
f. Failing to comply with—and thus violating—the THLL and its regulations;
g. Failing to adequately monitor the security of its networks and systems;
h. Failing to have in place mitigation policies and procedures;
i. Allowing unauthorized access to Plaintiffs' and Class Members' Sensitive Information;
j. Failing to detect in a timely manner that Plaintiffs' and Class Members' Sensitive Information had been compromised; and
k. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

186. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

187. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

188. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Sensitive Information.

189. Simply put, Defendant's negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

190. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

191. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to Plaintiffs and all Class Members.

Count III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

193. Defendant required Plaintiffs and Class Members to provide and entrust their Sensitive Information as a condition of obtaining services from Defendant and/or obtaining employment with Defendant.

194. Plaintiffs and Class Members paid money to Defendant, directly and/or indirectly, in exchange for goods, services, and/or employment, as well as Defendant's promise to protect their Sensitive Information from unauthorized disclosure.

195. Defendant promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' Sensitive Information would remain protected.

196. Implicit in the agreement between Defendant and Plaintiffs and Class Members was the obligation that both parties would maintain the Sensitive Information confidentially and securely.

197. Defendant had an implied duty of good faith to ensure that the Sensitive Information of Plaintiffs and Class Members in its possession was used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

198. Defendant had an implied duty to protect the Sensitive Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

199. Additionally, Defendant implicitly promised to retain this Sensitive Information only under conditions that kept such information secure and confidential.

200. Through its course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Sensitive Information.

201. Defendant solicited and invited Plaintiffs and Class Members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Sensitive Information to Defendant.

202. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class Members would not have provided their confidential Sensitive Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Sensitive Information for uses other than medical treatment, billing, and obtaining benefits from Defendant.

203. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to safeguard and protect Plaintiffs' and Class Members' Sensitive Information; failing to provide timely and accurate notice to Plaintiffs and Class Members that their Sensitive Information was compromised as a result of the Data Breach; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendant.

204. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

205. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

206. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

207. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

208. Defendant's failures to meet these promises constitute breaches of the implied contracts.

209. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiffs and Class Members that were of a diminished value.

210. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Sensitive Information in exchange for medical treatment and services and employment benefits.

211. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

212. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

Count IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

213. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

214. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claims.

215. Plaintiffs and Class Members conferred a monetary benefit on Defendant by paying money for healthcare services that relied on Defendant to render certain services, a portion of which was intended to have been used by Defendant for data security measures to secure Plaintiffs and Class Members' Sensitive Information. Plaintiffs and Class Members further conferred a benefit on Defendant by entrusting their Sensitive Information to Defendant from which Defendant derived profits.

216. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Sensitive Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

217. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

218. Defendant acquired the monetary benefit, PII, and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, as described herein, and failed to maintain adequate data security.

219. If Plaintiffs and Class Members knew that Defendant had not secured their Sensitive Information, they would not have agreed to give their money—or disclosed their data—to Defendant.

220. Plaintiffs and Class Members have no adequate remedy at law.

221. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their Sensitive Information is used; (3) the compromise, publication, and/or theft of their Sensitive Information; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Defendant's Data Breach.

222. The benefits that Defendant derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles

for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and data security practices alleged in this Complaint.

223. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Data Breach alleged herein.

Count V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

224. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

225. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Sensitive Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

226. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Sensitive Information.

227. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiffs and the Class in a reasonable and practicable period of time.

228. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Sensitive Information.

229. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

230. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Sensitive Information.

231. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

232. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

Count VI
Violation of the Texas Medical Practice Act ("TMPA")
Tex. Occ. Code §§ 159.001, *et seq.*
(On Behalf of Plaintiffs and the Class)

233. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

234. Under Tex. Occ. Code § 159.002(a)–(b), communications between a physician and a patient, relative to or in connection with any professional services as a physician to the patient, including records of the identity, diagnosis, evaluation, or treatment of a patient by a physician that is created or maintained by a physician, are confidential and privileged.

235. Under Tex. Occ. Code § 159.002(c), a person, including a hospital, that receives information from a confidential communication or record as described above and acts on the patient's behalf, may not disclose such information except to the extent that disclosure is consistent with the authorized purposes for which the information was first obtained.

236. Defendant's above-described wrongful actions, inaction and/or omissions that caused the Data Breach, caused the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI, and caused Plaintiffs and Class Members to suffer the resulting harm and damages collectively constitute the unauthorized release of confidential and privileged communications in violation of the TMPA. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and/or to recover their damages under Tex. Occ. Code § 159.009.

Count VII
Violation of the Texas Hospital Licensing Law
Tex. Health & Safety Code §§ 241.001, *et seq.*
(On Behalf of Plaintiffs and the Class)

237. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

238. Under Tex. Health & Safety Code § 241.151(2), "health care information" is any information, including payment information, recorded in any form or medium that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient.

239. Under Tex. Health & Safety Code § 241.152(a), except as authorized by Tex. Health & Safety Code § 241.153 (which does not apply here), a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

240. Under Tex. Health & Safety Code § 241.155, a hospital shall adopt and implement reasonable safeguards for the security of all health care information it maintains.

241. Defendant's above-described wrongful actions, inaction and/or omissions that caused the Data Breach, caused the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI, and caused Plaintiffs and Class Members to suffer the resulting harm and damages collectively constitute: (i) the unauthorized disclosure of Plaintiffs' and Class Members' health care information to unauthorized parties, and (ii) Defendant's failure to adopt and implement reasonable safeguards for the security of Plaintiffs' and Class Members' PHI entrusted to it—both of which are violations of the Texas Hospital Licensing Law. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and/or to recover their damages under Tex. Health & Safety Code § 241.156.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Sensitive Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Sensitive Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs under the common fund doctrine, and any other applicable law;

i) Costs and any other expense, including expert witness fees, incurred by Plaintiffs in connection with this action;

j) Pre- and post-judgment interest on any amounts awarded; and,

k) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: September 18, 2023

/s/ Joe Kendall

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
Tel: (214) 744-3000
Fax: (214) 744-3015
jkendall@kendalllawgroup.com

Christopher D. Jennings*
Tyler Ewigleben*
Laura Edmondson*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
tyler@yourattorney.com
ledmondson@yourattorney.com

Brian C. Gudmundson*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel: (612) 341-0400
Fac: (612) 341-0844
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

* *pro hac vice motions forthcoming*

Counsel for Plaintiffs and the Proposed Class